Automotive Safety Integrity Level

From Wikipedia, the free encyclopedia

For broader coverage of this topic, see ISO 26262 § Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis.

Automotive Safety Integrity Level (ASIL) is a risk classification scheme defined by the ISO 26262 - Functional Safety for Road Vehicles standard. This is an adaptation of the Safety Integrity Level (SIL) used in IEC 61508 for the automotive industry. This classification helps defining the safety requirements necessary to be in line with the ISO 26262 standard. The ASIL is established by performing a risk analysis of a potential hazard by looking at the Severity, Exposure and Controllability of the vehicle operating scenario. The safety goal for that hazard in turn carries the ASIL requirements.

There are four ASILs identified by the standard: ASIL A, ASIL B, ASIL C, ASIL D. ASIL D dictates the highest integrity requirements on the product and ASIL A the lowest.[1] Hazards that are identified as QM (*see below*) do not dictate any safety requirements.

Hazard Analysis and Risk Assessment [edit]

Because of the reference to SIL and because the ASIL incorporate 4 levels of hazard with a 5th non-hazardous level, it is common in descriptions of ASIL to compare its levels to the SIL levels and DO-178C Design Assurance Levels, respectively.

The determination of ASIL is the result of *hazard analysis and risk assessment*.[2] In the context of ISO 26262, a hazard is assessed based on the relative impact of hazardous effects related to a system, as adjusted for relative likelihoods of the hazard manifesting those effects. That is, each hazard is assessed in terms of severity of possible injuries within the context how much of the time a vehicle is exposed to the possibility of the hazard happening (refer ISO26262 definition of exposure) as well as the relative likelihood that a typical driver can act to prevent the injury (refer ISO26262 definitions of severity and controllability).[3]

In short, ASIL refers both to risk and to risk-dependent requirements (standard minimal risk treatment for a given risk). Whereas risk may be generally expressed as

$$\textbf{Risk} = (\textbf{expected loss in case of the accident}) \times (\textbf{probability of the accident occurring})$$

or

$$\textbf{Risk} = \textbf{Severity} \times (\textbf{Exposure} \times \textbf{Likelihood})$$[4][5]

ASIL may be similarly expressed as

$$\textbf{ASIL} = \textbf{Severity} \times (\textbf{Exposure} \times \textbf{Controllability})$$[6][7][8]

illustrating the role of Exposure and Controllability in establishing relative probability, which is combined with Severity to form an expression of risk.

Levels [edit]

The ASIL range from ASIL D, representing the highest degree of automotive hazard and highest degree of rigor applied in the assurance the resultant safety requirements, to QM, representing application with no automotive hazards and, therefore, no safety requirements to manage under the ISO 26262 safety processes. The intervening levels are simply a range of intermediate degrees of hazard and degrees of assurance required.

ASIL D [edit]

ASIL D, an abbreviation of *Automotive Safety Integrity Level D*, refers to the highest classification of initial hazard (injury risk) defined within ISO 26262 and to that standard's most stringent level of safety measures to apply for avoiding an unreasonable residual risk.[2] In particular, ASIL D represents likely potential for severely life-threatening or fatal injury in the event of a malfunction and requires the highest level of assurance that the dependent safety goals are sufficient and have been achieved.[2] An example of dangerous hazard that warrants the ASIL D level is loss of braking on all wheels.[9]

ASIL D is noteworthy, not only because of the elevated risk it represents and the exceptional rigor required in development, but because automotive electrical, electronic, and software suppliers make claims that their products have been certified or otherwise accredited to ASIL D,[10][11][12][13] ease development to ASIL D,[14] or are otherwise suitable to or supportive of development of items to ASIL D.[15][16][17] Any product able to comply with ASIL D requirements would also comply with any lower level.

ISO 26262 "highly recommends" the use of semi-formal modeling languages for ASIL D designs (Stateflow and SysML provide examples of such languages).[18] Executable validation using either prototyping or simulation is mandatory.[19]

ASIL C [edit]

Loss of braking for rear wheels only is less dangerous, this hazard is associated with ASIL C.[20] Another example of a less critical function that warrants the ASIL C rating is cruise control.[21]

For ASIL C designs the use of semi-formal modeling languages is highly recommended.[18] Executable validation using either prototyping or simulation is mandatory.[19]

ASIL B [edit]

ASIL B examples are headlights and brake lights.[21]

Modeling of the ASIL B design can rely on an informal languages.[18] This and other differences requirements make the cost difference between C and B to be the largest step across all the ASILs.[22]

ASIL A [edit]

ASIL A is the lowest rating of the functional safety. A typical example are tail lights (non-braking).[21] Less strict design walkthroughs can be used during the development (higher levels require more formal design inspections).[19]

QM [edit]

Referring to "Quality Management", the QM level means that all assessed risks are tolerable from a safety perspective (even if the manufacturer might want to address them from a customer satisfaction perspective, for example make sure the vehicle starts). So, safety assurance controls are unnecessary and standard quality management processes are sufficient for development.[23][2]

Decomposition [edit]

Designing an entire system to the rigorous standards of the higher levels of ASIL can be unwieldy, so ISO 26262 allows "decomposition": redundant subcomponents, each designed to a lower ASIL level, can be combined into a higher ASIL level design using higher-level methodologies. The subcomponents used in this way shall contain features that would allow higher-level integration. The frequently used notation for an ASIL X-level component that can be used as a part of an ASIL Y-level system is X(Y). For example, an A(B) component is designed at the ASIL A level of requirements, but is made to fit into ASIL B designs (this subcomponent is colloquially described as "B-ready"). ISO 26262 contains multiple examples of allowed decomposition scenarios, for example ASIL B = A(B) + A(B), i.e. two redundant B-ready ASIL A subcomponents can be combined into an ASIL B design. Headlights provide a natural example of such decomposition: there are at two of them, so they can be designed at ASIL A and combined into an ASIL B system as long as the combination is done properly (for example, it should not introduce a common point of failure).[24]

Comparison with Other Hazard Level Standards [edit]

Given ASIL is a relatively recent development, discussions of ASIL often compare its levels to levels defined in other well-established safety or quality management systems. In particular, the ASIL are compared to the SIL risk reduction levels defined in IEC 61508 and the Design Assurance Levels used in the context of DO-178C and DO-254. While there are some similarities, it is important to also understand the differences.

Approximate cross-domain mapping of ASIL

Domain	Domain-Specific Safety Levels							
Automotive (ISO 26262)	QM	ASIL A			ASIL B	ASIL C	ASIL D	-
General (IEC 61508)	-	SIL-1			SIL-2		SIL-3	SIL-4
Railway (CENELEC 50126/128/129)	-	SIL-1			SIL-2		SIL-3	SIL-4
Space (ECSS-Q-ST-80)	Category E	Category D			Category C		Category B	Category A
Aviation: airborne (ED-12/DO-178/DO-254)	DAL-E	DAL-D			DAL-C		DAL-B	DAL-A
Aviation: ground (ED-109/DO-278)	AL6	AL5			AL4	AL3	AL2	AL1
Medical (IEC 62304)	Class A	Class B					Class C	-
Household (IEC 60730)	Class A	Class B					Class C	-
Machinery (ISO 13849)	-	PL a	PL b	PL c	PL d	PL e	-	-
Agriculture (ISO 25119)	AgPL QM	AgPL a	AgPL b	AgPL c	AgPL d	AgPL e	-	-

IEC 61508 (SIL) [edit]

ISO 26262 is an extension of IEC 61508.[2] IEC 61508 defines a widely referenced Safety Integrity Level (SIL) classification. Unlike other functional safety standards, ISO 26262 does not provide normative nor informative mapping of ASIL to SIL; while the two standards have similar processes for hazard assessment, ASIL and SIL are computed from different perspectives.[25]

- An ISO 26262 ASIL is a *qualitative* statement of assessed risk, assessed in terms of three risk parameters in a qualitative way that leaves room for interpretation.[26][27][28][29][30][31]
- On the other hand, the IEC 61508 SIL employ *quantitative* target probability or frequency measures[27] of dangerous failures depending on the type of safety function.[32]

In the context of IEC 61508, higher risk applications require greater robustness to dangerous failures:

$$\textbf{probability of failure} < \frac{\textbf{Tolerable Risk}}{\textbf{Risk}}$$

That is, for a given Tolerable Risk, greater Risk requires more risk reduction, i.e., a smaller design target value for greater probability of dangerous failure. For a safety function operating in high demand or continuous mode of operation, SIL 1 is associated with a probability of dangerous failure limit of 10^{-5} per hour while SIL 4 is associated with a probability of dangerous failure rate limit of 10^{-9} per hour.

In commercial publications, ASIL D has been illustrated to align with SIL 3 and ASIL A is compared to SIL 1.[33]

SAE ARP4761 and SAE ARP4754 (DAL) [edit]

While it is more common to compare the ISO 26262 Levels D through QM to the Design Assurance Levels (DAL) A through E and ascribe those levels to DO-178C; these DAL are actually defined and applied through the definitions of SAE ARP4761 and SAE ARP4754. Especially in terms of the management of vehicular hazards through a Safety Life Cycle, the scope of ISO 26262 is more comparable to the combined scope of SAE ARP4761 and SAE ARP4754. Functional Hazard Assessment (FHA) is defined in ARP4761 and the DAL are defined in ARP4754. DO-178C and DO-254 define the design assurance objectives that must be accomplished for given DAL.

Unlike SIL, it is the case that both ASIL and DAL are statements measuring degree of hazard. DAL E is the ARP4754 equivalent of QM; in both classifications hazards are negligible and safety management is not required. At the other end, DAL A and ASIL D represent the highest levels of risk addressed by the respective standards, but they do not address the same level of hazard. While ASIL D encompasses at most the hazards of a loaded passenger van, DAL A includes the greater hazards of large aircraft loaded with fuel and passengers. Publications might illustrate ASIL D as equivalent to either DAL B, to DAL A, or as an intermediate level.

Associated standards [edit]

- ISO 26262
- SAE J2980

See also [edit]

- ASIL accuracy
- ARP4761
- ARP4754
- DO-178C
- DO-254
- IEC 61508

References [edit]

1. ^ http://www.ni.com/white-paper/13647/en/#toc2 National Instruments White Paper on ISO 26262 functional safety standard
2. ^ a b c d e *ISO 26262-3:2011(en) Road vehicles — Functional safety — Part 3: Concept phase* . International Standardization Organization.
3. ^ Hobbs, Chris; Lee, Patrick (July 9, 2013). *Understanding ISO 26262 ASILs* . Embedded Technologies. Penton Electronics Group. {{cite book}}: |magazine= ignored (help)
4. ^ Kinney, G. F.; Wiruth, A. D. (June 1976). *Practical Risk Analysis for Safety Management* . China Lake, California: Naval Weapons Center. "The risk score for some potentially hazardous situation is given numerically as the product of three factors: ."
5. ^ Chris Van der Cruyssen, *Risk Assessment Guidelines (sheet 4, Kinney method)* (PDF), economie, Belgian Federal Government
6. ^ Steve Hartley; Ireri Ibarra; Gunwant Dhadyalla (2011). *Functional Safety & Diagnostics of Hybrid Vehicles ("Severity x Exposure x Controllability = ASIL")* (PDF), pp. sheet 8
7. ^ *Smart & Compact Battery Cell Management System for Fully Electrical Vehicles (Sheet 9)* , STMicroelectronics[permanent dead link]
8. ^ *Hercules™ Safety Microcontrollers – 1 Day Safety MCU Workshop (sheet 25)*, Texas Instruments, Texas Instruments, 2013
9. ^ Pimentel 2019, p. 88.
10. ^ "News Release: Freescale Qorivva Microcontroller is First Automotive MCU to Receive ISO 26262 Functional Safety Standard Certification" . Freescale Semiconductor. September 6, 2012. Archived from the original on February 16, 2014. Retrieved January 23, 2015.

11. ^ "Programming Research certificated to ISO 26262 – ASIL D" . Programming Research. July 25, 2013. Retrieved April 25, 2017.
12. ^ "Certified tools for functional safety ("Certified for software development up ... ASIL D ···")" . IAR Systems. Retrieved August 6, 2013.
13. ^ "Press Release: Vector is the first supplier to deliver an ASIL-D certified AUTOSAR operating system" (PDF). Vector. 2013-02-18. Retrieved August 6, 2013.
14. ^ "SafeTI™ Design Packages for Functional Safety Applications" . Texas Instruments. Retrieved August 6, 2013.
15. ^ "Renesas Electronics Introduces 4th-Generation V850 Microcontrollers Series (··· developed for applications with the highest functional safety requirements (ASIL D/SIL3))" . Renesas Electronics. November 4, 2010. Retrieved August 6, 2013.
16. ^ "Microcontrollers foster ISO 26262 ASIL D-compliant system design" . THOMASNET. September 6, 2012. Retrieved August 6, 2013.
17. ^ *ARM® CortexTM-R4 Safety Microcontrollers (sheet 3)* (PDF), Vision Series Embedded, Arrow Electronics
18. ^ [a] [b] [c] Nakagawa & Antonino 2023, p. 91.
19. ^ [a] [b] [c] Nakagawa & Antonino 2023, p. 90.
20. ^ Pimentel 2019, p. 86.
21. ^ [a] [b] [c] Xie et al. 2023, p. 4.
22. ^ Pimentel 2019, p. 89.
23. ^ "A Guide to Automotive Safety Integrity Levels (ASIL)" . *jamasoftware.com*. Retrieved 2022-12-13. "The additional level, QM, stands for Quality Management and denotes non-hazardous items that require only standard quality management compliance."
24. ^ Frigerio, Vermeulen & Goossens 2019.
25. ^ "IEC 61508 Standard" . *ldra.com Standards Compliance*. LDRA. Retrieved 2022-12-13. "Other variations include the use of "ASILs" (Automotive Safety Integrity Levels) which are derived differently, with ASIL being a **qualitative measurement** of risk."
26. ^ Paul Chomicz (August 27-28, 2018). "Controlled Natural Language for Hazard Analysis and Risk Assessment" . *Proceedings of the Sixth International Workshop, CNL 2018*. Controlled Natural Language. Maynooth, Co. Kildare, Ireland. p. 42. Retrieved 2022-12-14. "The ISO 26262 standard **defines the three risk parameters in a qualitative way that leaves room for interpretation**."
27. ^ [a] [b] Perallos, Asier; Hernandez-Jayo, Unai; Onieva, Enrique; Garcia-Zuazola, Ignacio, eds. (2011). "Cyber Security Risk Analysis for Intelligent Transport Systems and In-vehicle Networks". *Intelligent Transport Systems : Technologies and Applications* . Wiley. pp. 87, 95. ISBN 9781118894767. Retrieved 2022-12-13. "The main difference between the ISO ASILs and IEC 61508 SIL is that the latter employ quantitative target probability measures while the ASILs are based on qualitative measures. .... In MISRA guidelines and ISO 262 this possibility is taken into account by means of a **qualitative** measure known as 'controllability' "
28. ^ Peter Björkman (2011). *Probabilistic Safety Assessment using Quantitative Analysis Techniques : Application in the Heavy Automotive Industry* (PDF). Uppsala University. Retrieved 2022-12-13. "In the area of functional safety, standards such as ISO 26262 assess safety mainly focusing on **qualitative assessment** techniques ..."
29. ^ *Concepts and Risk Analysis for a Cooperative and Automated Highway Platooning System* . Dependable Computing – EDCC 2020 Workshops. Munich, Germany. September 7, 2020. pp. 200-214. Retrieved 2022-12-14. "These [quantitative methods] state a maximal frequency of occurrence, rather than a mainly qualitative integrity target as in ISO 26262."
30. ^ "Concepts and Risk Analysis for a Cooperative and Automated Highway Platooning System" . *Proceedings*. Dependable Computing – EDCC 2020 Workshops. Munich, Germany. September 7, 2020. pp. 200 214. Retrieved 2022-12-14. "These state a maximal frequency of occurrence, rather than a mainly qualitative integrity target as in ISO 26262."
31. ^ Bernhard Kaiser (9 March 2016). "Functional Safety of Camera Monitor Systems". In Anestis Tersis (ed.). *Handbook of Camera Monitor Systems : The Automotive Mirror-Replacement Technology Based on ISO 16505* . Augmented Vision and Reality. p. 525. ISBN 9783319296111. Retrieved 2022-12-14. "...then the minimum requirement from ISO 26262 regarding safety analyses is to conduct a **qualitative** analysis (i.e. no need to calculate with failure probabilities ...."
32. ^ "IEC 61508 Standard" . *ldra.com Standards Compliance*. LDRA. Retrieved 2022-12-13. "The derivation of the SIL is covered in more detail in part 5 of the [61508] standard, "Examples of methods for the determination of safety integrity levels" which explains different **quantitative** approaches to the derivation of SILs."
33. ^ Frech, Marcus; Josef Mieslinger (2012). "Functional Safety Seminar & 1-Day HerculesTM Workshop". *Arrow Roadshow*: 63.

Sources [edit]

- Pimentel, J. (2019). *The Role of ISO 26262* . Automated Vehicle Safety. SAE International. ISBN 978-0-7680-0275-1. Retrieved 2023-07-28.
- Xie, G.; Zhang, Y.; Li, R.; Li, K.; Li, K. (2023). *Functional Safety for Embedded Systems* . CRC Press. ISBN 978-1-000-88131-8. Retrieved 2023-07-28.
- Frigerio, Alessandro; Vermeulen, Bart; Goossens, Kees (2019). *Component-Level ASIL Decomposition for Automotive Architectures*. 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). IEEE. doi:10.1109/dsn-w.2019.00021 .
- Nakagawa, E.Y.; Antonino, P.O. (2023). *Reference Architectures for Critical Domains: Industrial Uses and Impacts* . Springer International Publishing. ISBN 978-3-031-16957-1. Retrieved 2023-07-28.